

Algebraic Geometric Codes on Many Points from Kummer Extensions

D. Bartoli, L. Quoos, and G. Zini

Abstract

For Kummer extensions defined by $y^m = f(x)$, where $f(x)$ is a separable polynomial over the finite field \mathbb{F}_q , we compute the number of Weierstrass gaps at two totally ramified places. For many totally ramified places we give a criterion to find pure gaps at these points and present families of pure gaps. We then apply our results to construct n -points algebraic geometric codes with good parameters.

Keywords: Weierstrass semigroups, algebraic geometric codes, codes on many points, Kummer extensions.

MSC: 11G20, 14G50, 14H55.

1

1 Introduction

In the early eighties tools from algebraic geometry were applied by V. Goppa to construct linear codes using algebraic curves over finite fields, see [7]. Nowadays these codes are called algebraic-geometric codes, AG codes for short. The starting point in the construction of an AG code is a projective, absolutely irreducible, non singular algebraic curve \mathcal{X} of genus $g \geq 1$ defined over the finite field \mathbb{F}_q with cardinality q . Let $F = \mathbb{F}_q(\mathcal{X})$ be its function field with \mathbb{F}_q being the field of constants. Consider Q_1, \dots, Q_n pairwise distinct rational places

1

Daniele Bartoli is with the Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1 - 06123 Perugia - Italy, *email:* daniele.bartoli.

Giovanni Zini is with the Dipartimento di Matematica e Informatica “Ulisse Dini”, Università degli Studi di Firenze, Viale Morgagni 67/A - 50134 Firenze - Italy, *email:* gzini@math.unifi.it.

Luciane Quoos is with the Instituto de Matemática, Universidade Federal do Rio de Janeiro, Rio de Janeiro 21941-909 - Brazil, *email:* luciane@im.ufrj.br.

on F . Let $D = Q_1 + \cdots + Q_n$ and G be divisors such that Q_i is not in the support of G for $i = 1, \dots, n$. The linear code $C_\Omega(D, G)$ is defined by

$$C_\Omega(D, G) = \{(\text{res}_{Q_1}(\eta), \dots, \text{res}_{Q_n}(\eta)) \mid \eta \in \Omega(G - D)\} \subseteq \mathbb{F}_q^n,$$

where $\Omega(G - D)$ is the space of \mathbb{F}_q -rational differentials η on \mathcal{X} such that either $\eta = 0$ or $\text{div}(\eta) \succeq G - D$ and $\text{res}_{Q_j}\eta$ is the residue of η at Q_j .

The code $C_\Omega(D, G)$ has length n and dimension $k = i(G - D) - i(G)$ where $i(G)$ denotes the speciality index of the divisor G . We say that $C_\Omega(D, G)$ is an $[n, k, d]$ -code where d denotes the minimum distance of the code. One of the main features of this code is that its minimum distance d satisfies the classical Goppa bound, namely

$$d \geq \deg G - (2g - 2).$$

The integer $d^* = \deg G - (2g - 2)$ is usually called the *designed minimum distance*. One way to obtain codes with good parameters is to find codes that improve the designed minimum distance.

If $G = \alpha P$ for some rational place P on F and D is the sum of other rational places on \mathcal{X} , then the code $C_\Omega(D, G)$ is called an *one-point AG code*. Analogously, if $G = \alpha_1 P_1 + \cdots + \alpha_n P_n$ for n distinct rational places P_1, \dots, P_n on \mathcal{X} , then $C_\Omega(D, G)$ is called a *n-point AG code*. For a more detailed introduction to AG codes, see [12, 19].

For a one-point divisor $G = \alpha P$ on the function field F , Garcia, Kim, and Lax [5, 6] improved the designed minimum distance using the arithmetical structure of the Weierstrass semigroup at the rational place P . For a two-point divisor $G = \alpha_1 P_1 + \alpha_2 P_2$, Homma and Kim [10] introduced the notion of pure gaps and obtained similar results. By choosing α_1 and α_2 satisfying certain arithmetical conditions depending on the structure of the Weierstrass semigroup at P_1 and P_2 , they improved the designed minimum distance. Matthews [15] showed that for an arbitrary curve there exist two-point AG codes that have better parameters than any comparable one-point AG code constructed from the same curve. Finally, for divisors $G = \alpha_1 P_1 + \cdots + \alpha_n P_n$ at n distinct rational places on \mathcal{X} , results from the theory of generalized Weierstrass semigroups and pure gaps were obtained by Carvalho and Torres [2]. They have been used to obtain AG codes whose minimum distance beats the classical Goppa bound on the minimum distance, see Theorem 2.4.

Many applications and results on AG codes can be found for one- and two-point codes in [3, 4, 10, 18], and for n -point codes in [1, 2, 16]. The minimum distances of several AG codes have been studied in the case when \mathcal{X} is a Kummer curve. For instance, when \mathcal{X} is the Hermitian curve results can be found in [10, 11, 15], or a subcover of the Hermitian curve in [14], or a generalization of the Hermitian curve in [18].

In this paper we analyze n -point codes when F is a Kummer extension defined by $y^m = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is a separable polynomial of degree r coprime to m . We extend results by Castellanos, Masuda, and Quoos [3] on the Weierstrass semigroup at two rational places P_1 and P_2 . In particular, for a class of Kummer curves we explicitly compute the number of gaps at P_1, P_2 , see Theorem 3.2, generalizing a result by Matthews [15, Theorem 3.6]. For Kummer extensions, we also study the Weierstrass semigroup at many rational places under some hypothesis on the places. We give an arithmetic characterization of pure gaps (Propositions 4.1 and 4.2) and apply it to a large family of Kummer extensions to provide families of pure gaps (Propositions 4.3, 4.4, and 4.5). We obtain codes such that the Singleton defect $\delta = n + 1 - k - d$ is improved, see Remarks 4.6 and 4.7. We illustrate our results constructing AG codes on many points from the Hermitian function field, and observe that the best improvements on the minimum distance with respect to the corresponding ones in the MinT's Tables [17] are obtained by two- or three-point codes.

The paper is organized as follows. In Section 2 we set the notations and present the preliminary results on the Weierstrass semigroup at two and many points. In Sections 3 and 4 we consider a large class of Kummer curves. In particular, in Section 3 we study the Weierstrass semigroup at two totally ramified rational points and compute the number of gaps at them. In Section 4 we give an arithmetic characterization of pure gaps at many points which provides families of pure gaps. We apply them to the construction of AG codes improving the Singleton defect. We illustrate our results constructing AG codes on many points from the Hermitian curve, see Example 4.8.

2 Preliminary results

Let \mathcal{X} be a projective, absolutely irreducible, nonsingular algebraic curve of genus g defined over the finite field \mathbb{F}_q . Let $F = \mathbb{F}_q(\mathcal{X})$ be its function field with the field of constants \mathbb{F}_q . For a function z in F , (z) and $(z)_\infty$ stand for its principal and polar divisor, respectively. We denote by $\mathbb{P}(F)$ the set of places of F and by \mathcal{D}_F the free abelian group generated by the places of F . The elements D of \mathcal{D}_F are called *divisors* and can be written as

$$D = \sum_{P \in \mathbb{P}(F)} n_P P \quad \text{with } n_P \in \mathbb{Z}, n_P = 0 \text{ for almost all } P \in \mathbb{P}(F).$$

The degree of a divisor D is $\deg(D) = \sum_{P \in \mathbb{P}(F)} n_P \cdot \deg P$, where $\deg P$ is the degree of the place P over \mathbb{F}_q . Given a divisor $D \in \mathcal{D}_F$, the Riemann-Roch vector space associated to D is defined by $\mathcal{L}(D) := \{z \in F \mid (z) \geq -D\} \cup \{0\}$. We denote by $\ell(D)$ the dimension of $\mathcal{L}(D)$ as a vector space over the field of constants \mathbb{F}_q . From the Riemann-Roch Theorem, it follows

that, for divisors D such that $2g - 1 < \deg D$, we have $\ell(D) = \deg(D) + 1 - g$, see [19, Th. 1.5.17].

Let \mathbb{N} be the set of non-negative integers. For distinct rational places P_1, \dots, P_s on $\mathbb{P}(F)$, let

$$H(P_1, \dots, P_s) = \{(n_1, \dots, n_s) \in \mathbb{N}^s \mid \exists z \in F \text{ with } (z)_\infty = n_1 P_1 + \dots + n_s P_s\}$$

be the Weierstrass semigroup at P_1, \dots, P_s . The complement $G(P_1, \dots, P_s) = \mathbb{N}^s \setminus H(P_1, \dots, P_s)$ is always a finite set and its elements are called *Weierstrass gaps* at P_1, \dots, P_s . A gap can be characterized in terms of the dimension of certain Riemann-Roch spaces, more specifically, an s -tuple $(n_1, \dots, n_s) \in \mathbb{N}^s$ is a gap at P_1, \dots, P_s if and only if $\ell(\sum_{i=1}^s n_i P_i) = \ell((\sum_{i=1}^s n_i P_i) - P_j)$ for some $j \in \{1, \dots, s\}$.

For $s = 1$, the semigroup $H(P_1)$ is the well-known Weierstrass semigroup at one point on the curve and $G(P_1)$ has exactly g gaps. For $s \geq 2$, the number of gaps may vary depending on the choice of the points. When $s = 2$, the size of $G(P_1, P_2)$ was given by M. Homma [9] in terms of $G(P_1)$ and $G(P_2)$ as follows. Let $1 = a_1 < a_2 < \dots < a_g$ and $1 = b_1 < b_2 < \dots < b_g$ be the gap sequences at P_1 and P_2 , respectively. For $i = 1, \dots, g$, let $\gamma(a_i) = \min\{b \in G(P_2) \mid (a_i, b) \in H(P_1, P_2)\}$. By [13, Lemma 2.6], $\{\gamma(a_i) \mid i = 1, \dots, g\} = G(P_2)$. Therefore, there exists a permutation σ of the set $\{1, \dots, g\}$ such that $\gamma(a_i) = b_{\sigma(i)}$, and

$$\Gamma(P_1, P_2) = \{(a_i, b_{\sigma(i)}) \mid i = 1, \dots, g\}$$

is the graph of a bijective map γ between $G(P_1)$ and $G(P_2)$. Define

$$r(P_1, P_2) = |\{(x, y) \in \Gamma(P_1, P_2) \mid x < y, \gamma(x) > \gamma(y)\}|$$

the number of inversions for γ .

Theorem 2.1 ([9, Theorem 1]). *Under the above notation, the number of gaps at P_1, P_2 is*

$$|G(P_1, P_2)| = \sum_{i=1}^g a_i + \sum_{i=1}^g b_i - r(P_1, P_2).$$

A characterization of $\Gamma(P_1, P_2)$ is the following.

Lemma 2.2 ([9, Lemma 2]). *Let Γ' be a subset of $(G(P_1) \times G(P_2)) \cap H(P_1, P_2)$. If there exists a permutation τ of $\{1, \dots, g\}$ such that $\Gamma' = \{(a_i, b_{\tau(i)}) \mid i = 1, \dots, g\}$, then $\Gamma' = \Gamma(P_1, P_2)$.*

The Weierstrass semigroup $H(P_1, P_2)$ can be recovered from $\Gamma(P_1, P_2)$ as follows. For $\mathbf{x} = (a_1, b_1), \mathbf{y} = (a_2, b_2) \in \mathbb{N}^2$, define the *least upper bound* of \mathbf{x} and \mathbf{y} as $\text{lub}(\mathbf{x}, \mathbf{y}) = (\max\{a_1, a_2\}, \max\{b_1, b_2\})$. Then, by [13, Lemma 2.2],

$$H(P_1, P_2) = \{\text{lub}(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))\}. \quad (1)$$

We now introduce the important concept of pure gaps that will be used in the construction of AG codes. An s -tuple $(n_1, \dots, n_s) \in \mathbb{N}^s$ is a *pure gap* at P_1, \dots, P_s if

$$\ell\left(\sum_{i=1}^s n_i P_i\right) = \ell\left(\left(\sum_{i=1}^s n_i P_i\right) - P_j\right) \text{ for all } j = 1, \dots, s.$$

The set of pure gaps at P_1, \dots, P_s is denoted by $G_0(P_1, \dots, P_s)$. Clearly, a pure gap is always a gap.

Lemma 2.3 ([2, Lemma 2.5]). *An s -tuple (n_1, \dots, n_s) is a pure gap at P_1, \dots, P_s if and only if $\ell\left(\sum_{i=1}^s n_i P_i\right) = \ell\left(\sum_{i=1}^s (n_i - 1) P_i\right)$.*

Pure gaps can be used to improve the designed minimum distance of AG codes.

Theorem 2.4 ([2, Theorem 3.4]). *Let $P_1, \dots, P_s, Q_1, \dots, Q_n$ be pairwise distinct \mathbb{F}_q -rational points on \mathcal{X} and $(a_1, \dots, a_s), (b_1, \dots, b_s) \in \mathbb{N}^s$ be two pure gaps at P_1, \dots, P_s . Consider the divisors $D = Q_1 + \dots + Q_n$ and $G = \sum_{i=1}^s (a_i + b_i - 1) P_i$. Suppose that $a_i \leq b_i$ for all $i = 1, \dots, s$, and that each s -tuple $(c_1, \dots, c_s) \in \mathbb{N}^s$ with $a_i \leq c_i \leq b_i$ for $i = 1, \dots, s$, is also a pure gap at P_1, \dots, P_s . Then the minimum distance d of $C_\Omega(D, G)$ satisfies*

$$d \geq \deg(G) - (2g - 2) + s + \sum_{i=1}^s (b_i - a_i).$$

Hereafter we work on a Kummer extension $F = \mathbb{F}_q(x, y)/\mathbb{F}_q(x)$ defined by $y^m = f(x)$, $m \geq 2$, $p \nmid m$, $f(x)$ a separable polynomial of degree r in $\mathbb{F}_q[x]$ and $\gcd(m, r) = 1$. We denote by $P_1, \dots, P_s, P_\infty$ ($s \leq r$), the rational places of F which are totally ramified in the extension $F/\mathbb{F}_q(x)$, and P_∞ is the pole of x . The genus g of F is $(m - 1)(r - 1)/2$.

We use a result by Maharaj [14] to build up an arithmetic characterization of pure gaps at many points in a *Kummer extension*. Firstly we need the definition of the restriction of a divisor in a function field extension F/K . For any divisor D of F and any intermediate field $K \subseteq E \subseteq F$, write $D = \sum_{R \in \mathbb{P}(E)} \sum_{Q \in \mathbb{P}(F), Q|R} n_Q Q$. We define the restriction of D to E as

$$D|_E = \sum_{R \in \mathbb{P}(E)} \min \left\{ \left\lfloor \frac{n_Q}{e(Q|R)} \right\rfloor : Q|R \right\} R,$$

where $e(Q|R)$ is the ramification index of Q over R .

Theorem 2.5 ([14, Theorem 2.2]). *Let $F/\mathbb{F}_q(x)$ be a Kummer extension of degree m defined by $y^m = f(x)$. Then, for any divisor D of F that is invariant under the action of $\text{Gal}(F/\mathbb{F}_q(x))$, we have that*

$$\mathcal{L}(D) = \bigoplus_{t=0}^{m-1} \mathcal{L} \left([D + (y^t)] \Big|_{\mathbb{F}_q(x)} \right) y^t,$$

where $[D + (y^t)] \Big|_{\mathbb{F}_q(x)}$ denotes the restriction of the divisor $D + (y^t)$ to $\mathbb{F}_q(x)$.

3 The Weierstrass semigroup at two points

Let $F/\mathbb{F}_q(x)$ be a Kummer extension defined by $y^m = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is separable of degree r coprime with m , and consider the Weierstrass semigroup $H(P, Q)$ at two rational places of F which are totally ramified in $F/\mathbb{F}_q(x)$. As pointed out in Equation (1), the semigroup $H(P, Q)$ is related to the set $\Gamma(P, Q)$, and [3, Theorem 4.3] yields

$$\Gamma(P_\infty, P_1) = \left\{ (mr - mj - ri, i + m(j - 1)) \mid 1 \leq i \leq m - 1 - \left\lfloor \frac{m}{r} \right\rfloor, 1 \leq j \leq r - 1 - \left\lfloor \frac{ri}{m} \right\rfloor \right\},$$

where P_∞ is the unique pole of x and P_1 is another totally ramified place. We now compute $\Gamma(P_1, P_2)$, where P_1 and P_2 are two distinct rational places of F different from P_∞ and totally ramified in the extension $F/\mathbb{F}_q(x)$.

Proposition 3.1. *Let $F/\mathbb{F}_q(x)$ be a Kummer extension defined by $y^m = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is separable of degree r and $\gcd(r, m) = 1$. If P_1 and P_2 are two distinct totally ramified places of F different from P_∞ , then*

$$\Gamma(P_1, P_2) = \left\{ \left(mi - j, m \left(\left\lfloor \frac{rj}{m} \right\rfloor - i \right) - j \right) \mid 1 + \left\lfloor \frac{m}{r} \right\rfloor \leq j \leq m - 1, 1 \leq i \leq \left\lfloor \frac{rj}{m} \right\rfloor - 1 \right\}.$$

Proof. For $\iota \in \{1, 2\}$ let $\alpha_\iota \in \mathbb{F}_q$ be such that P_ι is the unique zero of $x - \alpha_\iota$ in F . Let i, j be positive integers and $k = \left\lfloor \frac{jr}{m} \right\rfloor - i$, so that $(i + k)m \geq jr$. By [3, Prop. 3.1], the pole divisor of $\frac{y^j}{(x - \alpha_1)^i (x - \alpha_2)^k}$ is $(mi - j)P_1 + (mk - j)P_2$. Also, for $j \in \{1 + \left\lfloor \frac{m}{r} \right\rfloor, \dots, m - 1\}$ and $h \in \{1, \dots, \left\lfloor \frac{rk}{m} \right\rfloor - 1\}$, we have that $(mh - j) \in G(P_1) \cap G(P_2)$ by [3, Th. 3.2]. Hence, the set

$$\Gamma' = \left\{ \left(mi - j, m \left(\left\lfloor \frac{rj}{m} \right\rfloor - i \right) - j \right) \mid 1 + \left\lfloor \frac{m}{r} \right\rfloor \leq j \leq m - 1, 1 \leq i \leq \left\lfloor \frac{rj}{m} \right\rfloor - 1 \right\}$$

is a subset of $G(P_1) \times G(P_2) \cap H(P_1, P_2)$. The cardinality of Γ' is

$$\begin{aligned} |\Gamma'| &= \sum_{k=1+\lfloor \frac{m}{r} \rfloor}^{m-1} \left(\left\lceil \frac{rk}{m} \right\rceil - 1 \right) = \left(\sum_{k=1+\lfloor \frac{m}{r} \rfloor}^{m-1} \left\lceil \frac{rk}{m} \right\rceil \right) - \left(m - \left\lfloor \frac{m}{r} \right\rfloor - 1 \right) \\ &= \left(\sum_{k=0}^{m-1} \left\lceil \frac{rk}{m} \right\rceil \right) - \left\lfloor \frac{m}{r} \right\rfloor - \left(m - \left\lfloor \frac{m}{r} \right\rfloor - 1 \right) = - \sum_{k=0}^{m-1} \left\lfloor \frac{-rk}{m} \right\rfloor - m + 1 \\ &= - (m-1)(-r-1)/2 - m + 1 = (m-1)(r-1)/2 = g, \end{aligned}$$

using [8, Page 94]. Therefore $\Gamma' = \Gamma(P_1, P_2)$ by Lemma 2.2. \square

From Proposition 3.1 we are able to compute the number of gaps at two totally ramified places in the case $m \equiv 1 \pmod{r}$.

Theorem 3.2. *Let $F/\mathbb{F}_q(x)$ be a Kummer extension defined by $y^m = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is separable of degree r and $\gcd(r, m) = 1$. Let $P_\infty \in \mathbb{P}(F)$ be the pole of x and $P_1 \neq P_2$ be two other totally ramified rational places in $F/\mathbb{F}_q(x)$. If $m = ur + 1$ for some integer u , then*

$$\begin{aligned} |G(P_1, P_2)| &= \frac{ur(r-1)(3ur^2 - 5ur + 4r + 4u - 2)}{12}, \text{ and} \\ |G(P_\infty, P_1)| &= \frac{ur(r-1)(3ur^2 - 3ur + 2r + 2)}{12}. \end{aligned}$$

Proof. By Proposition 3.1,

$$\Gamma(P_1, P_2) = \left\{ \left(mi - j, m \left(\left\lceil \frac{rj}{m} \right\rceil - i \right) - j \right) \mid 1+u \leq j \leq m-1, 1 \leq i \leq \left\lceil \frac{rj}{m} \right\rceil - 1 \right\}.$$

Setting $(i_0, j_0) \in \mathbb{N}^2$ with $1+u \leq j_0 \leq m-1$ and $1 \leq i_0 \leq \left\lceil \frac{rj_0}{m} \right\rceil - 1$; by Theorem 2.1, we need to count the number r_{i_0, j_0} of pairs $(i_1, j_1) \in \mathbb{N}^2$ such that

$$1+u \leq j_1 \leq ru, 1 \leq i_1 \leq \left\lceil \frac{rj_1}{m} \right\rceil - 1, m(i_0 - i_1) < j_0 - j_1, m \left(\left\lceil \frac{rj_1}{m} \right\rceil - \left\lceil \frac{rj_0}{m} \right\rceil + i_0 - i_1 \right) < j_1 - j_0. \quad (2)$$

For $h \in \{0, 1\}$ write $j_h = k_h u + t_h$ with $k_h \in \{1, \dots, r-1\}$ and $t_h \in \{1, \dots, u\}$. Then $\left\lceil \frac{rj_h}{m} \right\rceil = k_h + 1$. We split r_{i_0, j_0} in a number of cases:

- $j_1 = j_0$. Then (2) implies $i_0 + 1 \leq i_1 \leq k_1$.

- $j_1 > j_0$ and $k_1 = k_0$. Then (2) implies $1 \leq t_0 \leq u-1$, $t_1 \geq t_0+1$, and $i_0+1 \leq i_1 \leq k_1$.
- $j_1 > j_0$ and $k_1 > k_0$. Then (2) implies $i_0 + k_1 - k_0 \leq i_1 \leq k_1$.
- $j_1 < j_0$ and $k_1 < k_0$. Then (2) implies $1 \leq t_0, t_1 \leq u$, $1 \leq i_0 \leq k_1$, and $i_0 \leq i_1 \leq k_1$.
- $j_1 < j_0$ and $k_1 = k_0$. Then (2) implies $2 \leq t_0 \leq u$, $t_1 \leq t_0-1$, and $i_0+1 \leq i_1 \leq k_1$.

By direct computation, this yields

$$\begin{aligned}
r(P_1, P_2) &= \sum_{(i_0, j_0) \in \Gamma(P_1, P_2)} r_{i_0, j_0} = \sum_{k_0=1}^{r-1} \sum_{t_0=1}^u \sum_{i_0=1}^{k_0} (k_0 - i_0) + \sum_{k_0=1}^{r-1} \sum_{t_0=1}^{u-1} \sum_{t_1=t_0+1}^u \sum_{i_0=1}^{k_0} (k_0 - i_0) \\
&+ \sum_{k_0=1}^{r-2} \sum_{t_0=1}^u \sum_{k_1=k_0+1}^{r-1} \sum_{t_1=1}^u \sum_{i_0=1}^{k_0} (k_0 - i_0 + 1) + \sum_{k_0=2}^{r-1} \sum_{t_0=1}^u \sum_{k_1=1}^{k_0-1} \sum_{t_1=1}^u \sum_{i_0=1}^{k_1} (k_1 - i_0 + 1) \\
&+ \sum_{k_0=1}^{r-1} \sum_{t_0=2}^u \sum_{t_1=1}^{t_0-1} \sum_{i_0=1}^{k_0} (k_0 - i_0) = \frac{u^2(r-2)(r-1)r(r+3)}{12}.
\end{aligned}$$

Also, by [3, Th. 3.2], we have

$$\sum_{n \in G(P_1)} n = \sum_{n \in G(P_2)} n = \sum_{j=1+u}^{m-1} \sum_{i=1}^{\lceil \frac{rj}{m} \rceil - 1} (mi - j) = \sum_{k=1}^{r-1} \sum_{t=1}^u \sum_{i=1}^{k-1} ((ur+1)i - (ku+t)) \quad (3)$$

$$= \frac{ur(r-1)(2r^2u - 2ru + 2r - u - 1)}{12}. \quad (4)$$

Therefore we obtain

$$|G(P_1, P_2)| = \sum_{n \in G(P_1)} n + \sum_{n \in G(P_2)} n - r(P_1, P_2) = \frac{ur(r-1)(3r^2u - 5ru + 4r + 4u - 2)}{12}.$$

By [3, Theorem 4.3],

$$\Gamma(P_\infty, P_1) = \left\{ (mr - mj - ri, m(j-1) + i) \mid 1 \leq i \leq m-1-u, 1 \leq j \leq r-1 - \left\lfloor \frac{ri}{m} \right\rfloor \right\}.$$

For $(i_0, j_0) \in \mathbb{N}^2$ with $1 \leq i_0 \leq m-1-u$ and $1 \leq j_0 \leq r-1 - \left\lfloor \frac{ri_0}{m} \right\rfloor$, as above we need to count the number s_{i_0, j_0} of pairs $(i_1, j_1) \in \mathbb{N}^2$ such that

$$1 \leq i_1 \leq m-1-u, 1 \leq j_1 \leq r-1 - \left\lfloor \frac{ri_1}{m} \right\rfloor, m(j_1 - j_0) < r(i_0 - i_1), m(j_1 - j_0) < (i_0 - i_1). \quad (5)$$

For $h \in \{0, 1\}$ write $i_h = k_h u + t_h$, with $k_h \in \{0, \dots, r-2\}$ and $t_h \in \{1, \dots, u\}$. Then $\left\lfloor \frac{ri_h}{m} \right\rfloor = k_h$. We split s_{i_0, j_0} in a number of cases:

- $i_1 = i_0$. Then (5) implies $1 \leq j_1 \leq j_0 - 1$.
- $i_1 > i_0$, $k_1 > k_0$, and $t_1 \leq t_0$. Then (5) implies $k_1 - k_0 + 1 \leq j_0 \leq r - 1 - k_0$ and $1 \leq j_1 \leq k_0 - k_1 + j_0$.
- $i_1 > i_0$, $k_1 \geq k_0$, and $t_1 > t_0$. Then (5) implies $k_1 - k_0 + 2 \leq j_0 \leq r - 1 - k_0$ and $1 \leq j_1 \leq k_0 - k_1 - 1 + j_0$.
- $i_1 < i_0$ and $k_1 < k_0$. Then (5) implies $1 \leq j_1 \leq j_0$.
- $i_1 < i_0$, $k_1 = k_0$ and $t_1 < t_0$. Then (5) implies $1 \leq j_1 \leq j_0$.

By direct computation, this yields

$$\begin{aligned}
r(P_\infty, P_1) &= \sum_{(i_0, j_0) \in \Gamma(P_\infty, P_1)} s_{i_0, j_0} = \sum_{k_0=0}^{r-2} \sum_{t_0=1}^u \sum_{j_0=1}^{r-1-k_0} (j_0 - 1) \\
&+ \sum_{k_0=0}^{r-2} \sum_{t_0=1}^u \sum_{k_1=k_0+1}^{r-2} \sum_{t_1=1}^{t_0} \sum_{j_0=k_1-k_0+1}^{r-1-k_0} (k_0 - k_1 + j_0) \\
&+ \sum_{k_0=0}^{r-2} \sum_{t_0=1}^u \sum_{k_1=k_0}^{r-2} \sum_{t_1=t_0+1}^u \sum_{j_0=k_1-k_0+2}^{r-1-k_0} (k_0 - k_1 - 1 + j_0) \\
&+ \sum_{k_0=0}^{r-2} \sum_{t_0=1}^u \sum_{k_1=0}^{k_0-1} \sum_{t_1=1}^u \sum_{j_0=1}^{r-1-k_0} j_0 + \sum_{k_0=0}^{r-2} \sum_{t_0=1}^u \sum_{t_1=1}^{t_0-1} \sum_{j_0=1}^{r-1-k_0} j_0 = \frac{u(r-1)r(ur^2 + r - u - 5)}{12}.
\end{aligned}$$

Also, by [3, Th. 3.2], we have

$$\begin{aligned}
\sum_{n \in G(P_\infty)} n &= \sum_{i=1}^{m-1-u} \sum_{j=1}^{r-1-\lfloor \frac{ri}{m} \rfloor} (mr - mj - ri) \\
&= \sum_{k=0}^{r-2} \sum_{t=1}^u \sum_{j=1}^{r-1-k} (mr - mj - r(ku + t)) = \frac{ur(r-1)(2ur^2 - ur + r - 2)}{12},
\end{aligned}$$

and $\sum_{n \in G(P_1)} n$ was computed in 4. Therefore we obtain

$$|G(P_1, P_2)| = \sum_{n \in G(P_1)} n - \sum_{n \in G(P_2)} n + r(P_1, P_2) = \frac{ur(r-1)(3r^2u - 5ru + 4r + 4u - 2)}{12}.$$

□

Remark 3.3. If \mathcal{H} is the function field of the Hermitian curve defined by $y^{q+1} = x^q + x$ over \mathbb{F}_{q^2} , then Theorem 3.2 was already obtained in [15, Th. 3.6]. In fact, the places of \mathcal{H} which are totally ramified in $H/\mathbb{F}_{q^2}(x)$ are centered at Weierstrass points of \mathcal{H} .

4 Pure gaps at many points and codes

Throughout this section, $F/\mathbb{F}_q(x)$ is a Kummer extension defined by $y^m = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is separable of degree r and $\gcd(r, m) = 1$. Let $P_\infty \in \mathbb{P}(F)$ denote the unique pole of x , while P_1, \dots, P_s ($s \geq 1$) are other totally ramified places in $F/\mathbb{F}_q(x)$ different from P_∞ . In this section we give arithmetic conditions which characterize the pure gaps at P_1, \dots, P_s and at $P_\infty, P_1, \dots, P_s$. We use this characterization to determine explicit families of pure gaps at many points and apply it to construct AG codes with good parameters.

Proposition 4.1. *Under the above notation, let $s \leq r$. The s -tuple $(a_1, \dots, a_s) \in \mathbb{N}^s$ is a pure gap at P_1, \dots, P_s if and only if, for every $t \in \{0, \dots, m-1\}$, exactly one of the following two conditions is satisfied:*

- i) $\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{-rt}{m} \right\rfloor < 0$;
- ii) $\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{-rt}{m} \right\rfloor \geq 0$ and $\left\lfloor \frac{a_i+t}{m} \right\rfloor = \left\lfloor \frac{a_i-1+t}{m} \right\rfloor$, for all $i = 1, \dots, s$.

Proof. Let P_1, \dots, P_r be all the places of F which are totally ramified in $F/\mathbb{F}_q(x)$ except P_∞ , that is, P_i is the zero of $x - \alpha_i$, where $f(x) = \prod_{i=1}^r (x - \alpha_i)$ is the separable polynomial defining F by $y^m = f(x)$. Then the divisor of y in F is $(y) = \sum_{i=1}^r P_i - rP_\infty$, and hence, for any $t \in \{0, \dots, m-1\}$,

$$\sum_{i=1}^s a_i P_i + (y^t) = \sum_{i=1}^s (a_i + t) P_i + \sum_{i=s+1}^r t P_i - rt P_\infty.$$

Let $Q_1, \dots, Q_r, Q_\infty$ be the places of $\mathbb{F}_q(x)$ lying under $P_1, \dots, P_r, P_\infty$, respectively. Then

$$\left[\sum_{i=1}^s a_i P_i + (y^t) \right] \Big|_{K(x)} = \sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty.$$

Since

$$\mathcal{L}\left(\sum_{i=1}^s a_i P_i\right) = \bigoplus_{t=0}^{m-1} \mathcal{L}\left(\left[\sum_{i=1}^s a_i P_i + (y^t) \right] \Big|_{K(x)}\right) y^t,$$

by Theorem 2.5, we have

$$\begin{aligned}\ell\left(\sum_{i=1}^s a_i P_i\right) &= \sum_{t=0}^{m-1} \ell\left(\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty\right), \\ \ell\left(\sum_{i=1}^s (a_i-1) P_i\right) &= \sum_{t=0}^{m-1} \ell\left(\sum_{i=1}^s \left\lfloor \frac{a_i-1+t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty\right).\end{aligned}$$

By Lemma 2.3, (a_1, \dots, a_s) is a pure gap at P_1, \dots, P_s if and only if

$$\ell\left(\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty\right) - \ell\left(\sum_{i=1}^s \left\lfloor \frac{a_i-1+t}{m} \right\rfloor Q_i + \left\lfloor \frac{-rt}{m} \right\rfloor Q_\infty\right) = 0$$

for all $t \in \{0, \dots, m-1\}$. Since $\mathbb{F}_q(x)$ has genus 0, this happens if and only if, for all $t \in \{0, \dots, m-1\}$, either

$$\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{-rt}{m} \right\rfloor < 0$$

or

$$\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{-rt}{m} \right\rfloor \geq 0 \quad \text{and} \quad \sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor = \sum_{i=1}^s \left\lfloor \frac{a_i-1+t}{m} \right\rfloor.$$

□

Proposition 4.2. *Let $s \leq r$, then an $(s+1)$ -tuple $(a_0, a_1, \dots, a_s) \in \mathbb{N}^{s+1}$ is a pure gap at $P_\infty, P_1, \dots, P_s$ if and only if, for every $t \in \{0, \dots, m-1\}$, exactly one of the following two conditions is satisfied:*

- i) $\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{a_0-rt}{m} \right\rfloor < 0$;
- ii) $\sum_{i=1}^s \left\lfloor \frac{a_i+t}{m} \right\rfloor + \left\lfloor \frac{a_0-rt}{m} \right\rfloor \geq 0$, $\left\lfloor \frac{a_0-rt}{m} \right\rfloor = \left\lfloor \frac{a_0-1-rt}{m} \right\rfloor$ and $\left\lfloor \frac{a_i+t}{m} \right\rfloor = \left\lfloor \frac{a_i-1+t}{m} \right\rfloor$ for $i = 1, \dots, s$.

Proof. The proof is very similar to the proof of Proposition 4.1 and it is omitted. □

We now present three families of pure gaps at two points for $m \equiv 1 \pmod{r}$.

Proposition 4.3. *Suppose that $m = ur + 1$ for some integer u . Then*

- i) $((r-1)m - 2r, 1)$ is a pure gap at P_∞, P_1 ;
- ii) $((r-2)m - r, b)$, with $b \in \{1, \dots, u+1\}$ are pure gaps at P_∞, P_1 ;

iii) $((r-3)m+1+\alpha, 1+\beta)$, with $\alpha \in \{0, \dots, 2u-1\}$ and $\beta \in \{0, \dots, u-1\}$ are pure gaps at P_1, P_2 .

Proof. Let $a = rm - m - 2r$ and $t \in \{0, \dots, m-1\}$. We have $\lfloor \frac{a-rt}{m} \rfloor \neq \lfloor \frac{a-1-rt}{m} \rfloor$ if and only if m divides $a - rt = (r-1)m - r(t+2)$, that is $t = m-2$. Also, $t = m-2$ implies $\lfloor \frac{a-qt}{q^\ell+1} \rfloor = -1$. For any $t \in \{0, \dots, m-2\}$ we have $\lfloor \frac{1+t}{m} \rfloor = \lfloor \frac{t}{m} \rfloor = 0$. We conclude that for any $t \in \{0, \dots, m-2\}$ either $\lfloor \frac{a-rt}{m} \rfloor + \lfloor \frac{1+t}{m} \rfloor < 0$ or $\lfloor \frac{a-rt}{m} \rfloor + \lfloor \frac{1+t}{m} \rfloor = \lfloor \frac{a-1-rt}{m} \rfloor + \lfloor \frac{t}{m} \rfloor$. For $t = m-1$, $\lfloor \frac{a-rt}{m} \rfloor + \lfloor \frac{1+t}{m} \rfloor = -2+1 = -1 < 0$. By Proposition 4.2, $(a, 1)$ is a pure gap at P_∞, P_1 .

Now let $a = rm - 2m - r$, $b \in \{1, \dots, u+1\}$, and $t \in \{0, \dots, m-1\}$. We have that $\lfloor \frac{b+t}{m} \rfloor \in \{0, 1\}$, and $\lfloor \frac{b+t}{m} \rfloor = 1$ if and only if $t+b \geq m$, that is $t \in \{m-b, \dots, m-1\}$. In this case,

$$\left\lfloor \frac{a-rt}{m} \right\rfloor = \left\lfloor \frac{rm-2m-r-rt}{m} \right\rfloor = -2 + \left\lfloor \frac{rm-r-rt}{m} \right\rfloor = -2,$$

since $0 \leq rm - r - rt \leq r(b-1) \leq ru < m$. Hence, for all $t \in \{m-b, \dots, m-1\}$,

$$\left\lfloor \frac{a-rt}{m} \right\rfloor + \left\lfloor \frac{b+t}{m} \right\rfloor = -2 + 1 < 0.$$

For $t \in \{0, \dots, m-b-1\}$, we have that

$$\left\lfloor \frac{a-rt}{m} \right\rfloor + \left\lfloor \frac{b+t}{m} \right\rfloor = \left\lfloor \frac{a-rt}{m} \right\rfloor = \left\lfloor \frac{a-1-rt}{m} \right\rfloor = \left\lfloor \frac{a-1-rt}{m} \right\rfloor + \left\lfloor \frac{b-1+t}{m} \right\rfloor.$$

By Proposition 4.2, (a, b) is a pure gap at P_∞, P_1 .

Finally let $t \in \{0, \dots, m-1\}$ and $(a_\alpha, b_\beta) = ((r-3)m+1+\alpha, 1+\beta)$ with $\alpha \in \{0, \dots, 2u-1\}$ and $\beta \in \{0, \dots, u-1\}$. Note that $\lfloor \frac{a_\alpha+t}{m} \rfloor \neq \lfloor \frac{a_\alpha-1+t}{m} \rfloor$ if and only if $t = m-1-\alpha$, and $\lfloor \frac{b_\beta+t}{m} \rfloor \neq \lfloor \frac{b_\beta-1+t}{m} \rfloor$ if and only if $t = m-1-\beta$. Therefore,

$$\left\lfloor \frac{a_\alpha+t}{m} \right\rfloor + \left\lfloor \frac{b_\beta+t}{m} \right\rfloor \neq \left\lfloor \frac{a_\alpha-1+t}{m} \right\rfloor + \left\lfloor \frac{b_\beta-1+t}{m} \right\rfloor$$

if and only if $t = m-1-\alpha$ or $t = m-1-\beta$.

Suppose $t = m-1-\alpha$. Then

$$\begin{aligned} \left\lfloor \frac{-rt}{m} \right\rfloor &= -r + \left\lfloor \frac{r(1+\alpha)}{m} \right\rfloor = \begin{cases} -r, & \alpha \leq u-1 \\ -r+1, & \alpha \geq u \end{cases}, \\ \left\lfloor \frac{a_\alpha+t}{m} \right\rfloor &= r-2, \quad \left\lfloor \frac{b_\beta+t}{m} \right\rfloor = 1 + \left\lfloor \frac{\beta-\alpha}{m} \right\rfloor = \begin{cases} 1, & \text{for } \beta \geq \alpha \\ 0, & \text{for } \beta < \alpha \end{cases}. \end{aligned}$$

If $\alpha \geq u$, then

$$\left\lfloor \frac{-rt}{m} \right\rfloor + \left\lfloor \frac{a_\alpha + t}{m} \right\rfloor + \left\lfloor \frac{b_\beta + t}{m} \right\rfloor = (-r + 1) + (r - 2) + 0 < 0;$$

if $\alpha \leq u - 1$, then

$$\left\lfloor \frac{-rt}{m} \right\rfloor + \left\lfloor \frac{a_\alpha + t}{m} \right\rfloor + \left\lfloor \frac{b_\beta + t}{m} \right\rfloor \leq -r + (r - 2) + 1 < 0.$$

Suppose $t = m - 1 - \beta$. Then

$$\begin{aligned} \left\lfloor \frac{-rt}{m} \right\rfloor &= -r + \left\lfloor \frac{r(1 + \beta)}{m} \right\rfloor = -r, \\ \left\lfloor \frac{a_\alpha + t}{m} \right\rfloor &= r - 2 + \left\lfloor \frac{\alpha - \beta}{m} \right\rfloor = \begin{cases} r - 3, & \text{for } \alpha < \beta \\ r - 2, & \text{for } \alpha \geq \beta \end{cases}, \quad \left\lfloor \frac{b_\beta + t}{m} \right\rfloor = 1. \end{aligned}$$

Hence,

$$\left\lfloor \frac{-rt}{m} \right\rfloor + \left\lfloor \frac{a_\alpha + t}{m} \right\rfloor + \left\lfloor \frac{b_\beta + t}{m} \right\rfloor \leq -r + (r - 2) + 1 < 0.$$

The thesis follows from Proposition 4.1. \square

The following results present two families of pure gaps at many points for $m \equiv 1 \pmod{r}$.

Proposition 4.4. *Suppose that $m = ur + 1$ for some integer u , $s < r$, and $\alpha_i \in \{0, \dots, (s + 1 - i)u - 1\}$ for $i = 1, \dots, s$. Then $(a_1, \dots, a_s) = ((r - s - 1)m + 1 + \alpha_1, 1 + \alpha_2, \dots, 1 + \alpha_s)$ is a pure gap at P_1, \dots, P_s .*

Proof. Suppose there exist $t \in \{0, \dots, m - 1\}$ and $j \in \{1, \dots, s\}$ such that $\left\lfloor \frac{a_j + t}{m} \right\rfloor \neq \left\lfloor \frac{a_j - 1 + t}{m} \right\rfloor$. Thus $t = m - 1 - \alpha_j$. Let $h \in \{0, \dots, r - 2\}$ be such that $hu \leq \alpha_j < (h + 1)u$. We have

$$\begin{aligned} \left\lfloor \frac{-rt}{m} \right\rfloor &= \left\lfloor \frac{-r(m - 1 - \alpha_j)}{m} \right\rfloor = -r + \left\lfloor \frac{r(1 + \alpha_j)}{m} \right\rfloor = -r + h, \\ \left\lfloor \frac{a_1 + t}{m} \right\rfloor &= \left\lfloor \frac{(r - s - 1)m + 1 + \alpha_1 + m - 1 - \alpha_j}{m} \right\rfloor = \begin{cases} r - s, & \alpha_1 \geq \alpha_j \\ r - s - 1, & \alpha_1 < \alpha_j \end{cases}, \end{aligned}$$

and, for $i > 1$,

$$\left\lfloor \frac{a_i + t}{m} \right\rfloor = \left\lfloor \frac{1 + \alpha_i + m - 1 - \alpha_j}{m} \right\rfloor = \begin{cases} 0, & \alpha_i < \alpha_j \\ 1, & \alpha_i \geq \alpha_j \end{cases}.$$

Since

$$|\{i \in \{2, \dots, s\} : \alpha_i \geq \alpha_j\}| \leq s - 1 - |\{i \in \{2, \dots, s\} : (s + 1 - i)h - 1 < uh\}| = s - 1 - h,$$

this implies that

$$\left\lfloor \frac{-rt}{m} \right\rfloor + \left\lfloor \frac{a_1 + t}{m} \right\rfloor + \sum_{i=2}^m \left\lfloor \frac{a_i + t}{m} \right\rfloor \leq (-r + h) + (r - s) + (s - 1 - h) < 0.$$

Hence, the thesis follows by Proposition 4.1. \square

Proposition 4.5. *Suppose that $m = ur + 1$ for some integer u , $s < r - 1$, $\alpha \in \{0, \dots, s\}$, and $\beta_i \in \{0, \dots, iu - 1\}$ for $i \in \{1, \dots, s\}$. Then $(a_0, a_1, \dots, a_s) = ((r - s - 1)m - r + \alpha, 1 + \beta_1, \dots, 1 + \beta_s)$ is a pure gap at $P_\infty, P_1, \dots, P_s$.*

Proof. Let $t \in \{0, \dots, m - 2\}$, so that $t = ku + z$ with $k \in \{0, \dots, r - 1\}$ and $z \in \{0, \dots, u - 1\}$.

Suppose $\left\lfloor \frac{a_0 - rt}{m} \right\rfloor \neq \left\lfloor \frac{a_0 - 1 - rt}{m} \right\rfloor$. Then $m \mid (a_0 - rt) = (r - s - k - 1)m + \alpha + k - r(z + 1)$. Since $|\alpha + k - r(z + 1)| < m$, this implies $\alpha + k = r(z + 1)$, whence $r \mid (\alpha + k)$. As $0 \leq \alpha, k \leq r - 1$, and $r(z + 1) > 0$, we have that $\alpha + k = r$ and $z = 0$. Hence, $t = m - 1 - \alpha u$. Then

$$\left\lfloor \frac{a_0 - rt}{m} \right\rfloor = r - s - k - 1 = \alpha - s - 1.$$

Also, $1 + \beta_i + t \leq m - 1 - (\alpha - j)u$ for all i . Thus $a_j + t \leq m - 1$ for all $j \in \{1, \dots, \alpha\}$, so

$$\sum_{i=1}^s \left\lfloor \frac{a_i + t}{m} \right\rfloor \leq s - \alpha.$$

Therefore,

$$\sum_{i=1}^s \left\lfloor \frac{a_i + t}{m} \right\rfloor + \left\lfloor \frac{a_0 - rt}{m} \right\rfloor < 0.$$

Now suppose $\left\lfloor \frac{a_i + t}{m} \right\rfloor \neq \left\lfloor \frac{a_j - 1 + t}{m} \right\rfloor$ for some $j \in \{1, \dots, s\}$. Since $1 \leq a_j + t < 2m$, this implies $t = m - a_j = m - 1 - \beta_j$. Let $h \in \{0, r - 3\}$ be such that $hu \leq \beta_j < (h + 1)u$. We have

$$\left\lfloor \frac{a_0 - rt}{m} \right\rfloor = -s - 1 + \left\lfloor \frac{\alpha + r\beta_j}{m} \right\rfloor = -s - 1 + h$$

and, for $i > 0$,

$$\left\lfloor \frac{a_i + t}{m} \right\rfloor = 1 + \left\lfloor \frac{\beta_i - \beta_j}{m} \right\rfloor = \begin{cases} 0, & \beta_i < \beta_j \\ 1, & \beta_i \geq \beta_j \end{cases}.$$

Since

$$|\{i \in \{1, \dots, s\} : \beta_i \geq \beta_j\}| \leq s - |\{i \in \{1, \dots, s\} : ih - 1 < uh\}| = s - h,$$

this implies that

$$\left\lfloor \frac{a_0 - rt}{m} \right\rfloor + \sum_{i=1}^m \left\lfloor \frac{a_i + t}{m} \right\rfloor \leq (-s - 1 + h) + (s - h) < 0.$$

Finally, let $t = m - 1$. Then $\left\lfloor \frac{a_0 - rt}{m} \right\rfloor = -s - 1$ and $\left\lfloor \frac{a_i + t}{m} \right\rfloor = 1$ for all $i > 0$. Hence,

$$\left\lfloor \frac{a_0 - rt}{m} \right\rfloor + \sum_{i=1}^m \left\lfloor \frac{a_i + t}{m} \right\rfloor = (-s - 1) + s < 0.$$

The thesis follows by Proposition 4.2. \square

By means of Theorem 2.4, the results on pure gaps of this section can be used in order to obtain AG codes with good parameters. This is pointed out in the next remarks where we compute an upper bound for the Singleton defect of some codes.

Remark 4.6. For a Kummer extension $y^m = f(x)$, where $m = ur + 1$ and $s \leq r - 1$, consider the pure gaps $(a_1, \dots, a_s) = ((r - s - 1)m + 1, 1, \dots, 1)$ and $(b_1, \dots, b_s) = ((r - s - 1)m + su, (s - 1)u, \dots, u)$. Define the divisors $G = \sum_{i=1}^s (a_i + b_i - 1)P_i$ and D as the sum of n rational places of F different from P_1, \dots, P_s . Consider the $[n, k, d]$ -code $C_\Omega(D, G)$.

Suppose $2g - 2 < \deg G < n$, then $k = n + g - 1 - \deg G$. Since F has genus $g = ur(r - 1)/2$ we have by Proposition 4.4 and Theorem 2.4 that the Singleton defect $\delta = n + 1 - k - d$ satisfies

$$\delta \leq \frac{ur(r - 1) - us(s + 1)}{2}.$$

Remark 4.7. For a Kummer extension $y^m = f(x)$, where $m = ur + 1$ and $s \leq r - 2$ consider the pure gaps $(a_0, a_1, \dots, a_s) = ((r - s - 1)m - r, 1, \dots, 1)$ and $(b_0, b_1, \dots, b_s) = ((r - s - 1)m - r + s, u, \dots, su)$. Define the divisors $G = (a_0 + b_0 - 1)P_\infty + \sum_{i=1}^s (a_i + b_i - 1)P_i$ and D as the sum of n rational places of F different from $P_\infty, P_1, \dots, P_s$ and consider the $[n, k, d]$ -code $C_\Omega(D, G)$.

Suppose $2g - 2 < \deg G < n$, then $k = n + g - 1 - \deg G$. Since F has genus $g = ur(r - 1)/2$ we have by Proposition 4.5 and Theorem 2.4 that the Singleton defect δ satisfies

$$\delta \leq \frac{ur(r - 1) - us(s + 1)}{2} - s - 1.$$

Table 1: Results from Example 4.8

q^2	s	n	k	$d \geq$	improvement on d compared with [17]
16	1	64	48	12	1
16	2	63	55	6	0
25	1	125	97	20	1
25	2	124	106	12	1
49	2	342	295	30	3
49	3	341	307	20	1
64	1	512	430	56	1
64	2	511	445	42	3
64	3	510	459	30	2
64	4	509	472	20	0
81	3	727	656	42	3
81	4	726	671	30	0

We illustrate the results obtained by constructing codes on many points over the Hermitian function field.

Example 4.8. *The Hermitian function field \mathcal{H} is defined by the affine equation $y^{q+1} = x^q + x$, it is maximal over \mathbb{F}_{q^2} and has genus $g = q(q-1)/2$. We apply Remark 4.6 to construct $[n, k, d]$ -codes $C_\Omega(D, G)$ from \mathcal{H} . In this case we have $r = q, u = 1, 1 \leq s \leq q-1$ and $\deg G = 2(q-s-1)(q+1) + s(s+1)/2$. We choose s such that $2g-2 < \deg G < n$ with $n = q^3 + 1 - s$. Then*

$$k = n + g - 1 - \deg G = q^3 - \frac{3}{2}q^2 + \left(2s - \frac{1}{2}\right)q - \frac{s^2 - s}{2} + 2,$$

$$d \geq \deg G - (2g - 2) + s + \sum_{i=1}^s (b_i - a_i) = q^2 - (2s - 1)q + s^2 - s.$$

Table 1 summarizes results from Example 4.8. We list AG codes with the same or better parameters with respect to the corresponding ones in the MinT's Tables [17].

5 Acknowledgments

The research of D. Bartoli and G. Zini was partially supported by Ministry for Education, University and Research of Italy (MIUR) (Project PRIN 2012 “Geometrie di Galois e strutture di incidenza” - Prot. N. 2012XZE22K_005) and by the Italian National Group for

Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The second author L. Quoos was partially supported by CNPq, PDE grant number 200434/2015-2. This work was done while the author enjoyed a sabbatical at the Università degli Studi di Perugia leave from Universidade Federal do Rio de Janeiro.

References

- [1] C. Carvalho, and T. Kato, “Codes from curves with total inflection points,” *Des. Codes Cryptogr.*, vol. 45, pp. 359–364, 2007.
- [2] C. Carvalho, and F. Torres, “On Goppa codes and Weierstrass gaps at several points,” *Des. Codes and Cryptogr.*, vol. 35, pp. 211–225, 2005.
- [3] A.S. Castellanos, A.M. Masuda, and L. Quoos, “One- and two-point codes over Kummer extensions,” *IEEE Trans. Inform. Theory*, vol. 62, no. 9, pp. 4867–4872, 2016.
- [4] I.M. Duursma, and R. Kirov, “Improved two-point codes on Hermitian curves,” *IEEE Trans. Inf. Theory*, 57(7), 44694476, 2011.
- [5] A. Garcia, S.J. Kim, and R. Lax, “Consecutive Weierstrass gaps and minimum distance of Goppa codes,” *J. Pure Appl. Algebra*, vol. 84, pp. 199–207, 1993.
- [6] A. Garcia, and R. Lax, “Goppa codes and Weierstrass gaps,” in *Coding theory and algebraic geometry (Luminy, 1991)*, Lectures Notes in Math., vol. 1518, Springer, pp. 33–42, 1992.
- [7] V.D. Goppa, “Algebraic-geometric codes” (in Russian), *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 46, no. 4, pp. 762–781, 1982.
- [8] R.L. Graham, D.E. Knuth, and O. Patashnik, *Concrete Mathematics*. Addison-Wesley Publishing Company, 1989.
- [9] M. Homma, “The Weierstrass semigroup of a pair of points on a curve,” *Arch. Math. (Basel)*, vol. 67, no. 4, pp. 337–348, 1996.
- [10] M. Homma, and S.J. Kim, “Goppa codes with Weierstrass pairs,” *J. Pure Appl. Algebra*, vol. 162, no. 2–3, pp. 273–290, 2001.
- [11] M. Homma, and S.J. Kim, “The complete determination of the minimum distance of two-point codes on a Hermitian curve.’ *Designs, Codes and Cryptography* , vol. 40, no. 1, 5–24, 2006.

- [12] T. Høholdt, J. van Lint, and R. Pellikaan, “Algebraic Geometry Codes”, Elsevier, 1998.
- [13] S.J. Kim, “On the index of the Weierstrass semigroup of a pair of points on a curve,” *Arch. Math. (Basel)*, vol. 62, no. 1, pp. 73–82, 1994.
- [14] H. Maharaj, “Code construction on fiber products of Kummer covers,” *IEEE Trans. Inform. Theory*, vol. 50, no. 9, pp. 2169–2173, 2004.
- [15] G.L. Matthews, “Weierstrass Pairs and Minimum Distance of Goppa Codes,” *Des. Codes and Cryptogr.*, vol. 22, pp. 107–121, 2001.
- [16] G.L. Matthews, “The Weierstrass semigroup of an m -tuple of collinear points on a Hermitian curve,” in *Finite fields and applications*, Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, pp. 12–24, 2004.
- [17] MinT, “Online database for optimal parameters of (t, m, s) -nets, (t, s) -sequences, orthogonal arrays, and linear codes”, Online available at <http://mint.sbg.ac.at>.
- [18] A. Sepúlveda and G. Tizziotti, “Weierstrass semigroup and codes over the curve $y^q + y = x^{q^r+1}$,” *Adv. Math. Commun.*, vol. 8, no. 1, pp. 67–72, 2014.
- [19] H. Stichtenoth, *Algebraic Function Fields and Codes*, 2nd Edition, Graduate Texts in Mathematics, vol. 254, Springer, Berlin, 2009.